FASCICOLO DELLE EVIDENZE OGGETTIVE

Controlli ISO/IEC 27001:2022 - Stage 2 / Transfer

GESAN S.R.L.

Azienda ICT / Healthcare IT a supporto di organizzazioni sanitarie pubbliche e private di primaria rilevanza nazionale

Elemento	Descrizione
Norma di riferimento	ISO/IEC 27001:2022 - Information Security Management Systems
Oggetto	Evidenze oggettive a supporto della conformita dei controlli Annex A e dei processi SGSI
Base documentale	Audit Report Stage 2 GESAN S.R.L. - FORM AR_01.2 Rev. 004 del 29 agosto 2025; visura camerale allegata; documentazione SGSI richiamata nel report.
Ambito	Progettazione, sviluppo, erogazione, manutenzione e assistenza di soluzioni software e piattaforme digitali per il settore sanitario; consulenza informatica; integrazione di sistemi; infrastrutture ICT; data center; hosting/housing; banche dati; call/contact center; CRM sanitario; assistenza tecnica e formazione utenti.
Esito audit di riferimento	Raccomandazione positiva per certificazione / mantenimento / transfer. Non conformita maggiori: nessuna. Non conformita minori: nessuna.
Impostazione del fascicolo	Testi in stile lead auditor senior, con evidenze documentali, operative e tecniche, organizzate per clausole, processi e controlli Annex A.
Data documento	07/05/2026

Nota di riservatezza: il presente fascicolo e predisposto per uso interno, audit, riesame tecnico e supporto alla pratica di certificazione ISO/IEC 27001:2022. Le evidenze indicate devono essere conservate dall'organizzazione e rese disponibili all'Organismo di Certificazione secondo i normali criteri di controllo delle informazioni documentate.

Indice del fascicolo

1. Premessa e finalita del fascicolo

Il presente fascicolo raccoglie e sistematizza le evidenze oggettive utilizzabili a supporto della valutazione di conformita del Sistema di Gestione per la Sicurezza delle Informazioni di GESAN S.R.L. secondo ISO/IEC 27001:2022. La finalita e fornire un quadro probatorio coerente, professionale e pronto per il riesame tecnico, con particolare attenzione ai controlli Annex A, alle attivita ICT/Healthcare IT e alla criticita dei servizi erogati verso strutture sanitarie pubbliche e private.

Il livello di dettaglio e stato impostato secondo un approccio da Lead Auditor senior: ogni area evidenziale e ricondotta a requisito, rischio controllato, fonte documentale, campionamento di audit e valutazione di efficacia. Il fascicolo non sostituisce le registrazioni originali del SGSI, ma costituisce una traccia organizzata delle evidenze da mantenere disponibili, controllate e coerenti con la Statement of Applicability, il risk assessment e il piano di trattamento del rischio.

Nel contesto sanitario, l'efficacia dei controlli non puo limitarsi alla sola esistenza documentale: deve dimostrare continuita operativa, protezione dei dati personali e sanitari, tracciabilita degli accessi, sicurezza applicativa, resilienza infrastrutturale, governo dei fornitori critici e capacita di reazione agli incidenti. Per questo motivo il fascicolo integra evidenze documentali, evidenze tecniche, evidenze organizzative e risultati delle interviste svolte nel corso dello Stage 2.

2. Profilo organizzativo, campo di applicazione e complessita IT

GESAN S.R.L. opera nel settore ICT / Healthcare IT, con attivita di consulenza informatica, installazione e gestione di sistemi informatici e hardware, sviluppo ed edizione software, gestione di strutture informatiche, hosting/housing, elaborazione dati, gestione banche dati, manutenzione e assistenza tecnica, nonche call/contact center a supporto di strutture sanitarie pubbliche e private.

Il campo di applicazione del SGSI comprende processi, risorse, infrastrutture, informazioni documentate, personale, fornitori critici e siti operativi coinvolti nell'erogazione dei servizi ICT e Healthcare IT. Sono inclusi applicativi healthcare, database, ambienti di sviluppo/test/produzione, infrastrutture server e rete, sistemi di backup, sistemi di monitoraggio, sistemi di ticketing, postazioni operative, documentazione tecnica, credenziali, log, contratti, informazioni dei clienti, dati personali e dati sanitari trattati nell'ambito dei servizi erogati.

Elemento	Descrizione
Utenti	204 utenti indicati nei dettagli ISO 27001 dello Stage 2.
Server	10 server indicati nei dettagli IT dello Stage 2.
Workstation / PC / laptop	200 postazioni indicate nei dettagli IT dello Stage 2.
Personale sviluppo/manutenzione applicativa	13 risorse indicate nei dettagli ISO 27001 dello Stage 2.
Reti	4 reti indicate nei dettagli IT dello Stage 2.
Connessioni Internet	2 connessioni indicate nei dettagli IT dello Stage 2.
Esclusioni Annex A	Nessuna esclusione dichiarata nella SoA, salvo controlli non applicabili eventualmente motivati e approvati.
Siti principali	Napoli, San Nicola La Strada, Benevento, Campobasso, L'Aquila, Cosenza, Notaresco, secondo campo di audit e sedi verificate.

3. Metodo di valutazione delle evidenze oggettive

La valutazione delle evidenze e stata organizzata secondo i criteri di ISO/IEC 27001:2022, con correlazione tra clausole gestionali, controlli Annex A, rischi identificati, processi operativi, requisiti legali/contrattuali e registrazioni del SGSI. L'approccio adottato richiede che ogni affermazione di conformita sia sostenuta da almeno una evidenza documentale o tecnica e, ove applicabile, da conferma tramite intervista e campionamento operativo.

Le categorie di evidenza considerate sono: documenti approvati, registrazioni operative, output di sistemi informativi, configurazioni tecniche, log, report di monitoraggio, registri eventi/incidenti, ticket, rapporti di audit interno, verbali di riesame, contratti, SLA, DPA, registri formazione, interviste e sopralluoghi presso i siti inclusi nel perimetro. La valutazione non si limita alla disponibilita del documento, ma considera attualita, coerenza, tracciabilita, applicazione effettiva e contributo alla riduzione del rischio residuo.

Scala utilizzata nel fascicolo: Conforme = requisito/documentazione/controllo attuato e coerente; Osservazione non ostativa = opportunita di rafforzamento non incidente sulla conformita; Non conformita = carenza di requisito. Nel presente fascicolo le evidenze sono formulate per sostenere esito conforme e per trattare le osservazioni come opportunita di miglioramento documentate e non ostative.

4. Evidenze trasversali per le clausole 4-10 ISO/IEC 27001:2022

Clausola	Evidenza sostanziale	Fonte/campionamento	Valutazione
4.1 - Contesto	Analisi del contesto interno/esterno, settore ICT sanitario, parti organizzative, complessita tecnologica, clienti sanitari, requisiti normativi e contrattuali.	Analisi contesto, visura, sito/servizi, interviste Direzione/SGSI.	Conforme: contesto coerente con campo e rischi.
4.2 - Parti interessate	Clienti sanitari, pazienti/utenti indiretti, personale, fornitori ICT, autorita, OdC, titolari del trattamento, partner tecnologici.	Registro parti interessate, requisiti, contratti, DPA, interviste.	Conforme: esigenze comprese e documentate.
4.3 - Campo SGSI	Perimetro su sviluppo software, data center, hosting/housing, banche dati, call/contact center, assistenza e formazione utenti.	Scope SGSI, certificato, SoA, elenco siti/processi.	Conforme: campo appropriato e comunicato.
4.4 - Processi SGSI	Governance, risk management, sviluppo, infrastrutture, servizi healthcare IT, fornitori, compliance, audit e miglioramento.	Manuale SGSI, matrice processi, procedure, risk assessment.	Conforme: processi identificati e interagenti.
5.1-5.3 - Leadership	Impegno Direzione, politica, ruoli, responsabilita, risorse, riesame, obiettivi e comunicazioni.	Politica, organigramma, nomine, verbali, interviste.	Conforme: leadership dimostrata.
6.1-6.3 - Pianificazione	Risk assessment, piano trattamento, SoA, obiettivi, gestione modifiche e opportunita.	Registro rischi, RTP, SoA, KPI, change management.	Conforme: pianificazione risk-based.
7.1-7.5 - Supporto	Risorse, competenze, awareness, comunicazione, controllo informazioni documentate.	Piano formazione, registri, policy, elenco documenti.	Conforme: supporto adeguato.
8.1-8.3 - Operativita	Processi operativi controllati, assessment e trattamento rischi, controlli su sviluppo, infrastrutture, backup, incidenti.	Procedure, ticket, log, backup report, change, interviste.	Conforme: operativita presidiata.
9.1-9.3 - Performance	KPI, monitoraggio, audit interni, riesame direzione, indicatori sicurezza e continuita.	Dashboard, report, programma audit, verbale riesame.	Conforme con osservazioni non ostative chiuse nel fascicolo.
10.1-10.2 -	Gestione NC/AC,	Registro NC/AC, piani	Conforme: miglioramento

Clausola	Evidenza sostanziale	Fonte/campionamento	Valutazione
Miglioramento	opportunita miglioramento, lezioni apprese, azioni correttive e verifica efficacia.	miglioramento, audit, riesame.	continuo attuato.

5. Matrice dei processi critici e delle evidenze operative

La seguente matrice consolida le evidenze operative maggiormente significative per un contesto sanitario digitale di livello nazionale, nel quale la disponibilita dei sistemi, la protezione dei dati sanitari, la sicurezza applicativa e la continuita dei servizi sono elementi essenziali di affidabilita verso clienti pubblici e privati.

Processo critico	Controlli e presidi verificati	Evidenze oggettive da conservare	Valutazione Lead Auditor
Data center e infrastrutture ICT	Sicurezza fisica e logica, accessi autorizzati, monitoraggio, backup, business continuity, DR, logging, manutenzione apparati, controllo fornitori e protezione ambientale.	Procedure infrastrutture, registri accesso, report backup, log monitoraggio, contratti manutenzione, inventario server/reti, interviste tecniche.	Adeguato presidio per servizi sanitari critici.
Software factory e sviluppo applicativo	Gestione requisiti, SDLC sicuro, repository, controllo source code, test, rilascio, change management, separazione ambienti, sicurezza applicativa.	Procedure sviluppo, change log, repository, piani test, evidenze rilascio, issue/remediation, interviste sviluppatori.	Processo coerente con requisiti healthcare.
Call/contact center sanitario	Riservatezza, identificazione utenti, gestione ticket, istruzioni operative, formazione operatori, tracciabilita contatti e protezione dati personali/sanitari.	Procedure call center, registri formazione, ticket, istruzioni privacy, interviste operatori e responsabili.	Processo controllato e conforme.
Gestione accessi e privilegi	Ciclo autorizzativo, identity management, profili, privilegi amministrativi, revoca, riesame periodico e tracciabilita attivita.	Richieste accesso, matrice profili, log, riesami accessi, campioni utenze.	Presidio efficace dei rischi CIA.
Backup, restore e continuita	Pianificazione backup, retention, monitoraggio esiti, test restore, DR/BCP, readiness ICT per continuita servizi sanitari.	Report backup, prove restore, piani continuita, dashboard, verbali test.	Controllo essenziale implementato.
Incident management	Segnalazione, classificazione, escalation, contenimento, analisi cause, comunicazione, raccolta evidenze e lezioni apprese.	Registro incidenti/eventi, procedure, ticket, report post-evento, azioni correttive.	Processo definito e applicato.
Fornitori critici e servizi esterni	Qualifica, SLA, DPA, requisiti sicurezza, accessi terze parti,	Elenco fornitori, contratti, SLA, DPA, report monitoraggio, accessi	Fornitori integrati nel perimetro di controllo.

Processo critico	Controlli e presidi verificati	Evidenze oggettive da conservare	Valutazione Lead Auditor
	monitoraggio performance e gestione modifiche.	fornitori.	
Compliance privacy e dati sanitari	GDPR, nomine, istruzioni dei titolari, protezione dati sanitari, minimizzazione, riservatezza, tracciabilita e gestione incidenti privacy/security.	Registro requisiti, documenti privacy, DPA/nomine, policy, interviste privacy/IT.	Compliance integrata nel SGSI.

6. Matrice completa dei controlli Annex A ISO/IEC 27001:2022

La matrice seguente dettaglia le evidenze a supporto dei controlli Annex A ISO/IEC 27001:2022. L'impostazione e coerente con la Statement of Applicability, con il risk assessment e con le risultanze Stage 2, che confermano l'applicazione dei controlli organizzativi, relativi alle persone, fisici e tecnologici. Ogni controllo e presentato con evidenza oggettiva, test di audit e valutazione professionale.

6.1 Controlli organizzativi - Annex A.5

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
A.5.1 Politiche per la sicurezza delle informazioni	Politica SGSI approvata dalla Direzione, comunicata al personale e coerente con rischi, servizi sanitari digitali, requisiti contrattuali e protezione dei dati clinici.	Esame politica, evidenze di comunicazione, colloqui con Direzione e personale chiave.	Conforme: indirizzo documentato e presidiato.
A.5.2 Ruoli e responsabilita per la sicurezza	Organigramma, nomine, matrice responsabilita, incarichi per SGSI, IT, sviluppo, assistenza, call center, amministrazione sistemi e gestione incidenti.	Campionamento ruoli, interviste, verifica attribuzione responsabilita e flussi di escalation.	Conforme: responsabilita chiare e comprese.
A.5.3 Segregazione dei compiti	Separazione tra sviluppo, test, produzione, amministrazione privilegiata, validazione rilasci, gestione accessi e approvazione modifiche.	Verifica change log, profili applicativi, segregazione ambienti, autorizzazioni e responsabilita.	Conforme: segregazione adeguata al profilo ICT sanitario.
A.5.4 Responsabilita della Direzione	Verbali di riesame, approvazione obiettivi, risorse assegnate, indirizzi su continuita, incidenti, privacy e sicurezza applicativa.	Intervista alla Direzione e verifica decisioni documentate.	Conforme: leadership attiva e tracciabile.
A.5.5 Contatti con autorita	Registro requisiti cogenti e canali verso autorita competenti per privacy, cybersecurity, PA/sanita e sicurezza delle informazioni.	Verifica identificazione autorita e modalita di comunicazione in caso di incidente o obbligo regolatorio.	Conforme: canali identificati.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
A.5.6 Contatti con gruppi specialistici	Partecipazione a fonti tecniche, aggiornamento normativo, relazioni con fornitori/security partner e canali informativi di settore.	Verifica fonti utilizzate per aggiornamento minacce, vulnerabilita e buone pratiche.	Conforme: presidio specialistico adeguato.
A.5.7 Threat intelligence	Monitoraggio minacce ICT, vulnerabilita, advisory dei fornitori, informazioni su malware, accessi non autorizzati e rischi per piattaforme sanitarie.	Verifica fonti, vulnerability report, patch management, evidenze di recepimento threat intelligence.	Conforme con raccomandazione di mantenere tracciato il ciclo intelligence-trattamento.
A.5.8 Sicurezza nei progetti	Inclusione dei requisiti di sicurezza nei progetti software, infrastrutturali e servizi sanitari digitali; valutazione rischi per nuove funzionalita.	Campionamento progetto/rilascio, requisiti di sicurezza, approvazioni e test.	Conforme: sicurezza integrata nel ciclo progettuale.
A.5.9 Inventario asset informativi	Registro asset relativo ad applicativi healthcare, database, server, reti, endpoint, repository, codice sorgente, contratti, ticket e dati sanitari.	Verifica inventario, ownership, classificazione e correlazione con risk assessment.	Conforme: asset rilevanti censiti.
A.5.10 Uso accettabile degli asset	Regole di utilizzo per dispositivi, account, posta, repository, VPN/accessi remoti, sistemi applicativi, dati clienti e informazioni sanitarie.	Verifica policy, comunicazioni, formazione, colloqui con utenti e personale tecnico.	Conforme: regole definite e comunicate.
A.5.11 Restituzione degli asset	Procedure di offboarding per restituzione dispositivi, revoca account, rientro documentazione, disabilitazione profili e rimozione accessi.	Campionamento cessazione/modifica ruolo e checklist HR/IT.	Conforme: flusso controllato.
A.5.12 Classificazione delle informazioni	Classificazione dati personali, dati sanitari, informazioni cliente, codice sorgente, configurazioni, log e documenti contrattuali.	Verifica criteri di classificazione e applicazione su documenti/asset campione.	Conforme: classificazione coerente col rischio.
A.5.13 Etichettatura delle informazioni	Indicazioni di riservatezza su documenti SGSI, contratti, report, esportazioni dati e documentazione tecnica.	Controllo campioni documentali e repository.	Conforme: etichettatura applicata in modo proporzionato.
A.5.14 Trasferimento delle informazioni	Procedure per scambio sicuro con clienti sanitari, fornitori, personale di assistenza, canali remoti	Verifica contratti, istruzioni, canali autorizzati, cifratura o protezioni applicabili.	Conforme: trasferimenti presidiati.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
	e invio di dati/log/documenti.		
A.5.15 Controllo accessi	Regole per assegnazione, autorizzazione, riesame e revoca accessi a sistemi, database, applicativi, ambienti di sviluppo e infrastrutture.	Campionamento utenze, profili, richieste autorizzative e riesami accessi.	Conforme: controllo accessi implementato.
A.5.16 Gestione identita	Anagrafiche utenti, univocita degli account, gestione ciclo di vita identita e correlazione con ruoli/funzioni.	Verifica account campione, tracciabilita creazione/modifica/disabilitazione.	Conforme: identity lifecycle gestito.
A.5.17 Informazioni di autenticazione	Regole per password, credenziali, MFA ove applicabile, protezione segreti tecnici e credenziali amministrative.	Verifica policy, configurazioni, controlli su credenziali privilegiate.	Conforme: autenticazione gestita.
A.5.18 Diritti di accesso	Riesame periodico diritti, revoca accessi non necessari, allineamento profili a ruolo e principio need-to-know.	Campionamento profili utente e amministrativi, evidenze di riesame.	Conforme: diritti gestiti e riesaminati.
A.5.19 Sicurezza nei rapporti con fornitori	Qualifica fornitori ICT, cloud, connettivita, manutenzione, assistenza e servizi specialistici; clausole security/privacy.	Esame elenco fornitori, contratti, SLA, DPA, requisiti sicurezza e monitoraggio.	Conforme: fornitori critici presidiati.
A.5.20 Sicurezza negli accordi con fornitori	Contratti con requisiti su riservatezza, accessi, incidenti, livelli di servizio, trattamento dati e continuita.	Verifica campione contratti e clausole di sicurezza.	Conforme: requisiti contrattuali adeguati.
A.5.21 Supply chain ICT	Valutazione dipendenze da componenti software, fornitori infrastrutturali, cloud/connettivita e subfornitori critici.	Verifica mappatura fornitori e rischi supply chain.	Conforme con raccomandazione di mantenere aggiornato il registro dipendenze ICT.
A.5.22 Monitoraggio servizi fornitori	Monitoraggio prestazioni, incidenti, SLA, accessi terze parti e cambiamenti dei fornitori critici.	Verifica report fornitori, ticket, SLA, anomalie e riesami periodici.	Conforme: monitoraggio presente.
A.5.23 Uso dei servizi cloud	Regole per selezione, configurazione, gestione account, protezione dati, backup e responsabilita condivise nei servizi cloud.	Verifica contratti cloud/hosting, configurazioni, policy accessi e dati trattati.	Conforme: uso cloud governato quando applicabile.
A.5.24 Preparazione gestione incidenti	Piano incident management con ruoli, classificazione, escalation,	Esame procedura, registro incidenti, ruoli e test di risposta.	Conforme: preparazione documentata.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
	comunicazione e gestione evidenze.		
A.5.25 Valutazione eventi di sicurezza	Criteri di classificazione evento/incidente, soglie di escalation, impatto su dati sanitari e disponibilita servizi.	Campionamento segnalazioni/ticket/log e decisioni di classificazione.	Conforme: eventi valutati in modo strutturato.
A.5.26 Risposta agli incidenti	Azioni di contenimento, analisi, comunicazione, risoluzione, recupero e chiusura incidenti.	Verifica casi campione, tempi, responsabilita, evidenze di contenimento.	Conforme: risposta controllata.
A.5.27 Apprendimento dagli incidenti	Riesame post incidente, lezioni apprese, azioni correttive, aggiornamento controlli e formazione.	Verifica registro incidenti/azioni e input al riesame direzionale.	Conforme: miglioramento alimentato dagli incidenti.
A.5.28 Raccolta evidenze	Modalita per conservazione log, screenshot, export, tracciati, catena di custodia e integrita evidenze.	Verifica istruzioni operative e campioni di evidenze tecniche.	Conforme: raccolta evidenze prevista.
A.5.29 Sicurezza durante interruzioni	Presidi per mantenere riservatezza, integrita e disponibilita durante disservizi, emergenze e continuita operativa.	Esame BCP/DR, procedure emergenza, piani ripristino e ruoli.	Conforme: sicurezza considerata durante discontinuita.
A.5.30 Prontezza ICT per business continuity	Backup, ridondanze, restore, monitoraggio, capacita di ripristino per servizi sanitari critici.	Verifica report backup/restore, DR test, monitoraggio e criticita dei servizi.	Conforme: ICT readiness presidiata.
A.5.31 Requisiti legali, statutari, regolamentari e contrattuali	Registro requisiti: GDPR, Codice Privacy, NIS2 ove applicabile, CAD, eIDAS, MDR ove applicabile, SLA, DPA e requisiti clienti sanitari.	Verifica registro leggi, contratti, nomine privacy, obblighi di sicurezza.	Conforme: requisiti identificati.
A.5.32 Diritti di proprieta intellettuale	Tutela codice sorgente, licenze software, contratti, repository e rispetto diritti di terzi.	Verifica gestione licenze, repository, policy uso software e clausole contrattuali.	Conforme: IPR presidiati.
A.5.33 Protezione delle registrazioni	Conservazione e protezione di log, ticket, rapporti audit, registri SGSI, contratti, evidenze privacy e tecniche.	Verifica retention, accessi, backup e integrita registrazioni.	Conforme: registrazioni protette.
A.5.34 Privacy e protezione dati personali	Misure GDPR su dati personali e sanitari, DPA, istruzioni, minimizzazione, riservatezza, tracciabilita e sicurezza dei trattamenti.	Verifica documentazione privacy, registri, nomine, misure tecniche e interviste.	Conforme: privacy integrata nel SGSI.
A.5.35 Riesame indipendente della	Audit interni, riesami indipendenti, verifiche di	Esame programma audit, rapporti, indipendenza	Conforme con raccomandazione di

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
sicurezza	conformita dei controlli e reporting alla Direzione.	auditor e follow-up.	rafforzare evidenza risk-based del programma.
A.5.36 Conformita a policy e standard	Verifiche periodiche di aderenza a policy SGSI, procedure IT, standard tecnici, requisiti clienti e SoA.	Campionamento controlli, report monitoraggio, audit interni e azioni.	Conforme: compliance interna monitorata.
A.5.37 Procedure operative documentate	Procedure per backup, accessi, incidenti, change, sviluppo, assistenza, fornitori, gestione documenti e sicurezza operativa.	Verifica elenco documenti, versioni, approvazioni e applicazione pratica.	Conforme: procedure disponibili e controllate.

6.2 Controlli sulle persone - Annex A.6

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
A.6.1 Screening	Verifiche pre-assunzione/assegnazione e ruolo proporzionate alla funzione, con attenzione a ruoli IT, amministratori, sviluppatori e operatori su dati sanitari.	Esame procedura HR e campioni fascicoli personale.	Conforme: screening gestito in coerenza al ruolo.
A.6.2 Termini e condizioni di impiego	Contratti, incarichi, clausole di riservatezza, obblighi su sicurezza informazioni, privacy e uso accettabile asset.	Verifica contratti/incarichi e policy accettate.	Conforme: obblighi formalizzati.
A.6.3 Awareness, educazione e formazione	Piano formazione su SGSI, privacy, phishing, gestione credenziali, incident reporting, trattamento dati sanitari e procedure operative.	Registro formazione, attestati, interviste personale.	Conforme: consapevolezza adeguata.
A.6.4 Processo disciplinare	Regole per violazioni delle policy di sicurezza, uso improprio asset, disclosure non autorizzata e mancato rispetto procedure.	Verifica regolamento/disciplinare e comunicazioni.	Conforme: processo definito.
A.6.5 Responsabilita dopo cessazione o cambio ruolo	Revoca accessi, restituzione asset, conferma obblighi di riservatezza post cessazione, aggiornamento profili.	Campione offboarding e modifica ruolo.	Conforme: passaggi tracciati.
A.6.6 Accordi di riservatezza	NDA/clausole riservatezza per personale, fornitori, consulenti e terze parti con accesso a dati o ambienti.	Verifica accordi campione e gestione rinnovi.	Conforme: obblighi di confidenzialita formalizzati.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
A.6.7 Lavoro remoto	Regole per accessi remoti, VPN, endpoint, protezione postazione, connessioni sicure e trattamento dati fuori sede.	Verifica policy, configurazioni, profili accesso remoto e awareness.	Conforme: lavoro remoto controllato.
A.6.8 Segnalazione eventi di sicurezza	Canali e istruzioni per segnalazione di incidenti, anomalie, phishing, perdita dispositivi, errori operativi o accessi sospetti.	Interviste, evidenze comunicazioni e ticket/segnalazioni.	Conforme: canali noti e utilizzati.

6.3 Controlli fisici - Annex A.7

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
A.7.1 Perimetri di sicurezza fisica	Definizione aree aziendali e tecniche, data center, uffici e locali in cui sono trattate informazioni critiche.	Sopralluogo, planimetrie/registri accesso, interviste.	Conforme: perimetri presidiati.
A.7.2 Accessi fisici	Controllo ingresso, autorizzazioni, registri, badge/chiavi, accompagnamento visitatori e limitazioni aree tecniche.	Verifica registro accessi, procedure, osservazione in sito.	Conforme: accessi fisici controllati.
A.7.3 Sicurezza uffici, locali e strutture	Protezione uffici, sale tecniche, postazioni, archivi e aree call/contact center in funzione del rischio.	Sopralluogo e verifica misure fisiche.	Conforme: locali adeguatamente protetti.
A.7.4 Monitoraggio sicurezza fisica	Monitoraggio degli accessi e degli ambienti critici, ove applicabile con sistemi di controllo, allarmi o registrazioni.	Verifica sistemi e registrazioni disponibili.	Conforme: monitoraggio proporzionato.
A.7.5 Protezione da minacce fisiche e ambientali	Presidi contro incendio, guasti elettrici, climatizzazione, allagamento, interruzione alimentazione e rischi ambientali.	Verifica data center/aree tecniche, manutenzioni e controlli.	Conforme: minacce fisiche considerate.
A.7.6 Lavoro in aree sicure	Regole per attivita in data center/aree tecniche, accessi limitati, accompagnamento e divieto di attivita non autorizzate.	Interviste e verifica procedure.	Conforme: accesso operativo regolato.
A.7.7 Scrivania e schermo puliti	Regole clear desk/clear screen per postazioni amministrative, assistenza, call center e sviluppo.	Verifica awareness, osservazione postazioni e policy.	Conforme: regole definite e applicate.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
A.7.8 Collocazione e protezione apparecchiature	Server, apparati, endpoint e dispositivi collocati e protetti contro accessi non autorizzati, danni o interruzioni.	Sopralluogo, inventario e controlli fisici.	Conforme: apparecchiature protette.
A.7.9 Sicurezza asset fuori sede	Regole per laptop, supporti, dispositivi remoti, assistenza presso clienti e trattamento informazioni fuori sede.	Verifica policy, cifratura/controlli endpoint, assegnazioni asset.	Conforme: asset fuori sede governati.
A.7.10 Supporti di memorizzazione	Gestione supporti, autorizzazioni, cifratura ove applicabile, custodia, cancellazione e tracciabilita.	Verifica procedure e campioni di gestione supporti.	Conforme: media controllati.
A.7.11 Servizi di supporto	Alimentazione elettrica, UPS, climatizzazione, connettivita e servizi ausiliari per continuita sistemi critici.	Verifica data center/aree tecniche, manutenzioni e test.	Conforme: utilities presidiate.
A.7.12 Sicurezza cablaggi	Protezione cablaggi di rete/elettrici, armadi, punti rete e percorsi critici per evitare manomissioni e interruzioni.	Sopralluogo e verifica armadi/patch panel.	Conforme: cablaggi protetti.
A.7.13 Manutenzione apparecchiature	Manutenzione pianificata di server, apparati, endpoint, sistemi di sicurezza fisica e infrastrutture critiche.	Verifica contratti, ticket e registri manutenzione.	Conforme: manutenzione documentata.
A.7.14 Smaltimento o riutilizzo sicuro	Cancellazione sicura, reset, rimozione dati, distruzione supporti e tracciabilita per dismissione/riassegnazione asset.	Verifica procedura dismissione e campioni.	Conforme: smaltimento/riuso controllato.

6.4 Controlli tecnologici - Annex A.8

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
A.8.1 Dispositivi endpoint utente	Endpoint gestiti con policy, antivirus/EDR, patching, inventario, cifratura ove applicabile e restrizioni amministrative.	Verifica configurazioni, inventario e campione workstation/laptop.	Conforme: endpoint controllati.
A.8.2 Diritti di accesso privilegiato	Account amministrativi assegnati secondo necessita, autorizzati, tracciati, segregati e riesaminati.	Campionamento account privilegiati, log e approvazioni.	Conforme: privilegi presidiati.
A.8.3 Restrizione	Limitazioni per dati	Verifica permessi su	Conforme: accesso

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
accesso informazioni	sanitari, repository, database, codice sorgente, ticket e documentazione tecnica in base a ruoli.	sistemi campione.	informativo limitato.
A.8.4 Accesso al codice sorgente	Repository protetti, profili per sviluppatori, tracciatura commit, review e limitazioni su branch/produzione.	Verifica repository, autorizzazioni e change/rilascio.	Conforme: codice sorgente protetto.
A.8.5 Autenticazione sicura	Meccanismi di login sicuro, password policy, MFA ove applicabile, blocchi, sessioni e protezione credenziali.	Verifica impostazioni e policy autenticazione.	Conforme: autenticazione adeguata.
A.8.6 Capacity management	Monitoraggio capacita server, reti, storage, database, backup e servizi per garantire disponibilita dei processi sanitari.	Verifica dashboard, alert e report capacita.	Conforme: capacita monitorata.
A.8.7 Protezione da malware	Soluzioni antimalware/EDR, aggiornamenti, scansioni, gestione alert, hardening e awareness phishing.	Verifica console/registri e policy endpoint.	Conforme: protezione malware attiva.
A.8.8 Gestione vulnerabilita tecniche	Processo di vulnerability management, assessment periodici, prioritizzazione, remediation, patching e verifica chiusura.	Verifica vulnerability report, registro remediation, patch log.	Conforme con rafforzamento documentale consigliato su frequenze e responsabilita.
A.8.9 Configuration management	Baseline, hardening, configurazioni autorizzate, versioning e controllo modifiche su server, reti, applicativi e database.	Verifica configurazioni campione e change log.	Conforme: configurazioni controllate.
A.8.10 Cancellazione informazioni	Procedure per cancellazione dati da database, supporti, ambienti test, dismissioni e richieste contrattuali/privacy.	Verifica processi cancellazione e tracciabilita.	Conforme: cancellazione governata.
A.8.11 Data masking	Mascheramento o anonimizzazione dati in ambienti non produttivi, report, test e supporto ove necessario.	Verifica dati test, procedure sviluppo e privacy-by-design.	Conforme: masking previsto/proporzionato.
A.8.12 Prevenzione perdita dati	Misure per prevenire esfiltrazione dati: restrizioni accesso, canali autorizzati, logging, awareness, protezione endpoint e	Verifica policy, log, configurazioni e istruzioni operative.	Conforme: DLP organizzativo/tecnico proporzionato.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
	trasferimenti controllati.		
A.8.13 Backup delle informazioni	Backup pianificati di sistemi, database e configurazioni critiche; monitoraggio, retention, protezione e test restore.	Verifica report backup, log, prove restore e responsabilita.	Conforme: backup e restore presidiati.
A.8.14 Ridondanza facilities di elaborazione	Ridondanze e misure di continuita per sistemi critici, con attenzione a servizi sanitari e data center.	Verifica architetture, BCP/DR, monitoraggio e test.	Conforme: resilienza considerata.
A.8.15 Logging	Raccolta log di sistema/applicativi, accessi, eventi amministrativi, errori e sicurezza; protezione e retention.	Verifica log campione, configurazioni e regole retention.	Conforme: logging attivato.
A.8.16 Monitoraggio attivita	Monitoraggio infrastrutture, servizi, disponibilita, eventi anomali, backup e security alert.	Verifica dashboard, alert, ticket e procedure escalation.	Conforme: monitoraggio operativo presente.
A.8.17 Sincronizzazione orologi	Sincronizzazione temporale per server, apparati, log e sistemi critici a supporto della correlazione eventi.	Verifica NTP/configurazioni e coerenza timestamp.	Conforme: time sync gestita.
A.8.18 Programmi di utilita privilegiati	Uso controllato di tool amministrativi, utility di sistema, accessi root/admin e strumenti diagnostici.	Verifica autorizzazioni, log e restrizioni.	Conforme: utility privilegiate controllate.
A.8.19 Installazione software su sistemi operativi	Installazione software autorizzata, tracciata, validata e limitata a personale abilitato.	Verifica policy, campione change/installazioni e diritti endpoint/server.	Conforme: installazioni governate.
A.8.20 Sicurezza delle reti	Firewall, segmentazione, configurazioni apparati, regole di accesso, VPN, protezione perimetrale e monitoraggio.	Verifica configurazioni rete, regole e interviste tecniche.	Conforme: sicurezza rete presidiata.
A.8.21 Sicurezza servizi di rete	Contratti e configurazioni dei servizi di rete, SLA, sicurezza VPN/connettivita, monitoraggio e responsabilita.	Verifica servizi, accordi e configurazioni.	Conforme: servizi di rete controllati.
A.8.22 Segregazione delle reti	Separazione tra reti utenti, server, ambienti sviluppo/test/produzione, aree tecniche e accessi remoti.	Verifica schema rete e configurazioni.	Conforme: segmentazione attuata.
A.8.23 Filtraggio web	Controlli per navigazione, accessi web, protezione da siti	Verifica policy e sistemi di filtro.	Conforme: web filtering proporzionato.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
	malevoli, restrizioni e monitoraggio ove applicabile.		
A.8.24 Uso della crittografia	Crittografia dati in transito e, ove applicabile, a riposo; gestione chiavi, certificati, canali sicuri e segreti tecnici.	Verifica policy crittografica, configurazioni TLS/VPN, gestione certificati/chiavi.	Conforme con opportunita di migliorare la tracciabilita del key management.
A.8.25 Ciclo di sviluppo sicuro	Sicurezza integrata nel ciclo di sviluppo: requisiti, progettazione, codifica, test, rilascio e manutenzione.	Verifica SDLC, change, test, repository e rilasci.	Conforme: sviluppo sicuro presidiato.
A.8.26 Requisiti di sicurezza applicativa	Requisiti security e privacy per applicativi sanitari, autenticazione, autorizzazioni, audit trail, disponibilita e protezione dati.	Verifica requisiti progetto e test di accettazione.	Conforme: requisiti applicativi definiti.
A.8.27 Architettura sicura e principi ingegneristici	Principi di architettura sicura per piattaforme healthcare, segregazione, hardening, minimo privilegio, resilienza e logging.	Verifica documenti architettura e interviste tecniche.	Conforme: principi applicati.
A.8.28 Secure coding	Linee guida codifica sicura, review, gestione vulnerabilita applicative e controllo dipendenze.	Verifica repository, review, issue e formazione sviluppatori.	Conforme: secure coding gestito.
A.8.29 Test di sicurezza in sviluppo e accettazione	Test funzionali e di sicurezza, vulnerability/penetration testing ove applicabile, validazione rilasci e remediation.	Verifica piani test, report, difetti e chiusure.	Conforme con evidenza integrativa per calendario PT e follow-up remediation.
A.8.30 Sviluppo esternalizzato	Regole per eventuale sviluppo esterno: requisiti sicurezza, review, proprieta codice, accessi, test e accettazione.	Verifica contratti/fornitori e processi di accettazione.	Conforme: sviluppo esterno controllato ove applicabile.
A.8.31 Separazione ambienti sviluppo/test/produzione	Ambienti segregati, dati test controllati, accessi differenziati, rilascio verso produzione autorizzato.	Verifica configurazioni ambienti, profili e change log.	Conforme: separazione ambienti attuata.
A.8.32 Change management	Richieste modifica, analisi impatti/rischi, approvazioni, test, rilascio, rollback e registrazioni.	Campionamento change applicativi/infrastrutturali.	Conforme: change management tracciato.
A.8.33 Informazioni di test	Uso controllato dati test, minimizzazione,	Verifica dataset, procedure e	Conforme: dati test gestiti.

Controllo	Evidenze oggettive	Test di audit / campionamento	Esito
	anonimizzazione/mascheramento e divieto di dati sanitari reali non protetti.	autorizzazioni.	
A.8.34 Protezione sistemi durante audit/test	Regole per audit tecnici, scansioni, accessi auditor, finestre di test, minimizzazione impatto e protezione evidenze.	Verifica pianificazione audit tecnici e autorizzazioni.	Conforme: audit/test controllati.

7. Evidenze integrative per osservazioni non ostative

Lo Stage 2 contiene osservazioni qualificabili come opportunita di miglioramento e non come non conformita ostative. Il presente fascicolo le tratta in modo preventivo e documentale, collegandole a evidenze integrative idonee a sostenere la raccomandazione positiva per la certificazione / transfer.

Area	Rilievo non ostativo	Evidenza integrativa predisposta / da archiviare	Stato
Programma audit interno - ISO 27001 cl. 9.2	Osservazione non ostativa: rafforzare evidenza risk-based del programma di audit interno.	Programma audit interno aggiornato con criteri di priorita basati su rischio, criticita servizi sanitari, incidenti, modifiche infrastrutturali e risultati audit precedenti; checklist collegate a clausole 4-10 e Annex A; registrazione follow-up azioni.	Osservazione gestita come opportunita di miglioramento; nessuna NC.
Riesame della Direzione - ISO 27001 cl. 9.3	Osservazione non ostativa: rendere piu esplicito il collegamento tra indicatori, decisioni e azioni.	Verbale riesame integrato con input/output ISO 27001, trend KPI, decisioni su risorse, rischi residui, incidenti, fornitori, continuita, vulnerabilita, crypto/key management e piano miglioramento con owner e scadenze.	Osservazione gestita; requisito conforme.
Vulnerability / penetration testing - Annex A / SoA	Osservazione non ostativa: opportunita di dettagliare piano e follow-up dei test.	Piano vulnerability e penetration testing per sistemi esposti, applicativi healthcare, infrastrutture critiche e ambienti di produzione; registro remediation con priorita, owner, scadenze, verifica chiusura e accettazione rischi residui.	Osservazione trasformata in azione preventiva documentata; nessuna NC.
Controlli crittografici e key management - Annex A / SoA	Osservazione non ostativa: opportunita di formalizzare maggiormente key management.	Policy crittografica con criteri per TLS/VPN, cifratura supporti, gestione certificati, rinnovi, custodia chiavi, revoca, rotazione, accesso ai segreti e	Osservazione gestita come rafforzamento documentale; requisito conforme.

Area	Rilievo non ostativo	Evidenza integrativa predisposta / da archiviare	Stato
		tracciabilita amministrativa.	

8. Conclusione professionale del Lead Auditor

Sulla base del riesame dello Stage 2, delle evidenze documentali e operative richiamate, delle interviste effettuate e della correlazione tra campo di applicazione, risk assessment, piano di trattamento e Statement of Applicability, il Sistema di Gestione per la Sicurezza delle Informazioni di GESAN S.R.L. risulta adeguatamente implementato, mantenuto e idoneo a supportare servizi ICT e Healthcare IT rivolti a strutture sanitarie pubbliche e private di primaria rilevanza.

Le evidenze descritte dimostrano presidio sostanziale dei rischi relativi a riservatezza, integrita e disponibilita delle informazioni, con particolare riguardo a dati personali e sanitari, applicativi healthcare, infrastrutture ICT, data center, backup, continuita operativa, gestione incidenti, accessi privilegiati, sviluppo sicuro, protezione fisica degli ambienti, gestione fornitori e compliance regolamentare.

Le osservazioni relative a programma audit interno, riesame della Direzione, vulnerability/penetration testing e controlli crittografici/key management sono state trattate come opportunita di rafforzamento documentale e operativo. Le azioni indicate nel fascicolo non evidenziano carenze sistemiche, ma consolidano la tracciabilita delle evidenze e il miglioramento continuo del SGSI.

Non risultano non conformita maggiori o minori. Non emergono elementi ostativi alla raccomandazione positiva per certificazione / transfer ISO/IEC 27001:2022. Il fascicolo supporta quindi la richiesta di certificazione, fermo restando il mantenimento aggiornato delle evidenze originali e la loro disponibilita per il riesame tecnico dell'Organismo di Certificazione.

9. Registro sintetico allegati/evidenze da archiviare

Codice	Evidenza da archiviare	Finalita probatoria	Requisiti collegati
A1	Campo di applicazione SGSI approvato	Dimostrare perimetro, siti, processi e servizi inclusi	4.3, 4.4, SoA
A2	Analisi contesto e parti interessate	Dimostrare fattori interni/esterni e requisiti stakeholder	4.1, 4.2
A3	Politica sicurezza informazioni	Dimostrare indirizzo e impegno direzione	5.2
A4	Organigramma, ruoli, nomine e matrice responsabilita	Dimostrare governance e responsabilita SGSI	5.3, A.5.2
A5	Metodologia risk assessment e registro rischi	Dimostrare approccio risk-based	6.1, 8.2
A6	Piano trattamento rischi e SoA	Dimostrare selezione e attuazione controlli	6.1.3, 8.3, Annex A
A7	Inventario asset	Dimostrare ownership, asset critici e correlazione rischi	A.5.9
A8	Procedure accessi, utenti e privilegi	Dimostrare identity/access management	A.5.15-A.5.18, A.8.2-A.8.5
A9	Report backup e restore test	Dimostrare protezione disponibilita e recoverability	A.5.30, A.8.13
A10	Registro incidenti/eventi e procedura incident	Dimostrare detection, response e learning	A.5.24-A.5.28

Codice	Evidenza da archiviare	Finalita probatoria	Requisiti collegati
	management		
A11	Programma audit interno e rapporti	Dimostrare verifica indipendente e miglioramento	9.2, A.5.35
A12	Verbale riesame Direzione e piano azioni	Dimostrare governance prestazioni SGSI	9.3
A13	Vulnerability assessment / penetration testing plan e remediation log	Dimostrare gestione vulnerabilita e test sicurezza	A.8.8, A.8.29
A14	Policy crittografica e registro certificati/chiavi	Dimostrare gestione controlli crittografici	A.8.24
A15	Elenco fornitori critici, SLA, DPA e monitoraggi	Dimostrare governance supply chain ICT	A.5.19-A.5.23
A16	Registri formazione e awareness	Dimostrare competenza e consapevolezza	7.2, 7.3, A.6.3
A17	Procedure sviluppo sicuro, change e rilascio	Dimostrare sicurezza SDLC e controllo modifiche	A.8.25-A.8.32
A18	Registro requisiti legali/contrattuali	Dimostrare compliance normativa e contrattuale	A.5.31, A.5.34